

Come gestire i dati trattati dalle intelligenze artificiali

Quando si parla di [intelligenza artificiale nelle fabbriche](#), spesso si sottovaluta un aspetto importante: il trattamento dei dati sensibili, e le ricadute rispetto al GDPR (Regolamento generale sulla protezione dei dati).

È noto che sistemi come i software AI per la diagnostica medica trattano dati sensibili, e che anche software come chat GTP possono avere a che fare con dati personali. Si tende però a pensare che nelle fabbriche questo problema non ci sia.

Ma è davvero così?

Non esattamente. Pensiamo ad esempio ad un software di AI che aiuta a organizzare l'addestramento e la formazione degli operai. Nel sistema potrebbero essere inseriti dati personali come nomi e cognomi, codice fiscale...

Oppure, ancora, pensiamo ai DPI che rilevano parametri vitali come il battito cardiaco, la temperatura corporea, la saturazione dell'ossigeno o l'elettrocardiogramma per monitorare che gli operatori non siano vittime di incidenti.

Un altro esempio può riguardare invece il mondo dei produttori di macchinari, che possono decidere di integrare un chatbot di assistenza personalizzata nella macchina. Anche questo chatbot potrebbe richiedere i dati personali della persona con cui si interfaccia (almeno nome e

cognome).

Cosa succede poi a quei dati? Vengono effettivamente trattati e conservati ai sensi del GDPR?

Proviamo a capire quali sono le domande da porsi per rispettare la legge.

[Questo articolo deriva da una serie di ragionamenti condivisi con Silvia Zuanon, avvocato d'impresa. Se ti interessa trovi il [webinar completo qui](#)]

Leggi anche: [Chatbot e intelligenza artificiale per l'assistenza tecnica dei macchinari industriali](#)

Intelligenze artificiali e protezione dei dati sensibili: legittimità del trattamento



La prima domanda da porsi è: i dati forniti ai sistemi di AI possono essere trattati legalmente?

Secondo il GDPR, il trattamento di dati personali è lecito solo se esiste una base giuridica valida, come il consenso dell'utente, l'adempimento di un contratto o il legittimo interesse del titolare del trattamento.

Facciamo un esempio.

Sei un'azienda che fornisce un servizio di assistenza e metti a disposizione un chatbot per rispondere alle richieste, almeno in una prima fase. In questo caso il trattamento dei dati è considerato lecito in quanto stai adempiendo ad un contratto. In altre parole, i dati servono per poter offrire il servizio che metti a disposizione.

Questo vale per ogni tipologia di trattamento dati: anche se inserisci dei nominativi nel gestionale aziendale hai degli obblighi legati al GDPR. Nel caso delle intelligenze artificiali, però, il trattamento è automatizzato. È quindi necessario informare l'utente al momento della raccolta dei dati e specificare che questi potrebbero essere elaborati anche tramite intelligenza artificiale.

Trasferimento dei dati sensibili verso server di terze parti e verso altri Paesi

Un altro aspetto cruciale da considerare è: dove vengono conservati i dati? I dati finiscono solo sul gestionale interno dell'azienda o vengono inviati su un server esterno?

Molto spesso la risposta è la seconda: i dati finiscono su un server esterno, dove restano per 30 giorni e poi vengono (in teoria) cancellati.

Se i dati finiscono su server esterni sorgono ulteriori obblighi di conformità, specialmente se i server sono situati fuori dall'UE. Tuttavia spesso le aziende non sanno dove si trovano i server o come i dati vengano realmente trattati. Se questi server non sono situati in Europa, e sono ad esempio negli Stati Uniti, il rischio di violazioni aumenta. Diventa allora fondamentale adottare misure contrattuali e tecniche per garantire la conformità al GDPR.

Ad esempio, se un'azienda utilizza un sistema di intelligenza artificiale sviluppato da un fornitore esterno all'Unione Europea, come accade di

solito, l'azienda dovrebbe stipulare un accordo di nomina del fornitore come responsabile esterno del trattamento, specificando i limiti e le modalità di utilizzo dei dati.

Quando un'azienda affida a terzi il trattamento dei dati personali, entra infatti in gioco la nomina del responsabile esterno al trattamento dati. Questo processo implica la redazione di un accordo formale o di un atto di nomina, in cui il responsabile esterno si impegna a rispettare precise regole stabilite dal titolare del trattamento, come previsto dal Regolamento Generale sulla Protezione dei Dati (GDPR). Tali regole garantiscono che il trattamento dei dati resti conforme alle normative in vigore, proteggendo i diritti delle persone coinvolte.

Il contratto formale che designa le parti terze come responsabili del trattamento dati dovrà:

- definire chiaramente come i dati verranno trattati;
- garantire la conformità del fornitore al GDPR;
- prevedere l'adozione di misure tecniche e organizzative adeguate.

Inoltre, se il server di appoggio si trova in un Paese al di fuori dell'Unione Europea, bisognerà verificare che la normativa del Paese in questione offra garanzie adeguate. Ciò può avvenire attraverso accordi internazionali, che certificano che il livello di protezione dei dati è equivalente a quello europeo.

In sintesi: a cosa fare attenzione

I rischi più comuni legati al trattamento di dati sensibili da parte dell'AI sono:

- dati personali inseriti in AI pubbliche o non controllate – se l'AI non offre garanzie sul trattamento dei dati, questo potrebbe rappresentare una violazione del GDPR;
- condivisione non autorizzata con terzi – è fondamentale sapere dove i dati vengono conservati e chi vi ha accesso;
- trattamento non trasparente: gli interessati devono sempre sapere come e perché i loro dati vengono usati.

Tutti questi rischi possono essere bilanciati, la normativa sul trattamento dei dati prevede delle soluzioni che si possono adottare per contrastarli. Prima di tutto occorre però essere consapevoli dei pericoli, in modo da trovare poi le strategie giuste per affrontarli.

PS. Se ti interessa il tema dell'AI nel mondo industriale, ti consiglio anche questo articolo: [AI Act e macchinari industriali: come si applica il Regolamento sull'intelligenza artificiale al mondo delle fabbriche?](#)